数理解析研究所講究録 1240 巻 2001 年 224-232

「2整数が互いに素になる確率」の確率論的見方
— 数値実験による予想の検証 —

杉田 洋 (Hiroshi Sugita)
九大・数理学研究院 (Faculty of Mathematics, Kyushu University)
高信 敏 (Satoshi Takanobu)
金沢大・理学部 (Faculty of Science, Kanazawa University)

1. [3] の結果

Dirichlet による「2整数が互いに素になる確率」に関する定理がある:

定理 1 (Dirichlet の定理).

$$\lim_{N\to\infty}\frac{1}{N^2}\#\left\{1\le x,y\le N\,;\,\gcd(x,y)=1\right\}=\frac{6}{\pi^2}.$$

ここで $\#A$ は A の要素の個数, $\gcd(x,y)$ は x と y の最大公約数 (greatest common divisor) を表わす.

これを我々, 確率論者に馴染みのある形に書き直すと

$$\lim_{N\to\infty}\frac{1}{N^2}\sum_{m,n=1}^{N}X(m,n)=\frac{6}{\pi^2}$$

となる. ここで $X:\mathbf{Z}\times\mathbf{Z}\to\mathbf{R}$ は

$$X(x,y):=\begin{cases}1 & \text{if}\quad \gcd(x,y)=1,\\ 0 & \text{if}\quad \gcd(x,y)>1\end{cases}$$

により定義されるものである. さらに $\left\{X(x+m,y+n)\right\}_{(m,n)\in\mathbf{Z}\times\mathbf{Z}}$ を確率場と考えて

$$S_N(x,y):=\frac{1}{N^2}\sum_{m,n=1}^{N}X(x+m,y+n)$$

とするならば

$$\lim_{N\to\infty}S_N(x,y)=\frac{6}{\pi^2},\qquad {}^{\forall}(x,y)\in\mathbf{Z}\times\mathbf{Z}$$

となることが上のことから容易に分かる.

我々は [3] において, この収束が「確率論における大数の強法則」と捉えられることに気づいた.

このことを述べるため, いくつかの言葉の準備が必要となる:

定義 1. 素数 p に対して，$\mathbb{Z}$ 上の p 進距離 d_p を次のように導入する:

$$d_p(x,y) := \min\left\{\frac{1}{p^k}\,;\, p^k | x-y,\ \text{i.e.,}\ p^k \text{ は } x-y \text{ を割り切る}\right\}, \quad x,y\in\mathbb{Z}.$$

d_p による $\mathbb{Z}$ の完備化を $\mathbb{Z}_p$ と表わす．$(\mathbb{Z}_p, d_p)$ は compact 距離空間となる．$\mathbb{Z}$ 上の代数演算 '+' と '×' は連続的に $\mathbb{Z}_p$ に拡張され，よって $(\mathbb{Z}_p, d_p)$ は環 (これを p 進整数環という) となる．これを '+' に関して見れば，compact abel 群であるから，一般論より正規化された Haar 測度，即ち，平行移動不変な Borel 確率測度が一意的に存在する．これを λ_p と表わす．

定義 2. $\{p_i\}_{i=1}^{\infty}$, $2 = p_1 < p_2 < \cdots$, は素数を小さい順に並べた列とする．

$$\widehat{\mathbb{Z}} := \prod_{i=1}^{\infty} \mathbb{Z}_{p_i}, \quad \lambda := \prod_{i=1}^{\infty} \lambda_{p_i}$$

とおく．$x = (x_i), y = (y_i) \in \widehat{\mathbb{Z}}$ に対して

$$d(x,y) := \sum_{i=1}^{\infty} \frac{1}{2^i} d_{p_i}(x_i, y_i),$$

$$x + y := (x_i + y_i),$$

$$xy := (x_i y_i)$$

と定義するとき，$\widehat{\mathbb{Z}}$ は環 (これを有限整 adele 環とよぶ)，$(\widehat{\mathbb{Z}}, d)$ は compact 距離空間となり，演算 '+' と '×' は連続となる．特にこれは '+' に関して compact abel 群であり，その正規化された Haar 測度は λ に他ならない．

定義 3. (i) $\mathbb{Z}$ を対角線集合 $\left\{(n,n,\ldots) \in \mathbb{Z}\times\mathbb{Z}\times\cdots\,;\, n \in \mathbb{Z}\right\} \subset \widehat{\mathbb{Z}}$ と同一視すると，$\mathbb{Z}$ は $\widehat{\mathbb{Z}}$ の部分環，そして $\widehat{\mathbb{Z}}$ で稠密となる．(しかし $\lambda(\mathbb{Z}) = 0$ である！)

(ii) 「$\widehat{\mathbb{Z}}$ の元 x を自然数 m で割ったときの余り $x \bmod m$」を

$$x \bmod m = k\ (\in \{0,1,\ldots,m-1\}) \underset{\text{def}}{\Longleftrightarrow} x - k \in m\widehat{\mathbb{Z}}$$

により定義する．明らかに x が $\mathbb{Z}$ の元のときは，これは通常のものと一致する．

(iii) $x, y \in \widehat{\mathbb{Z}}$ に対して「最大公約数 $\gcd(x,y)$」を

$$\gcd(x,y) = \sup\left\{m \in \mathbb{N}\,;\, (x \bmod m) = (y \bmod m) = 0\right\}$$

により定義する．$x, y \in \mathbb{Z}$ のときは，通常の定義と一致する．

以上のもとで，先の X, 及び S_N を $\widehat{\mathbb{Z}}\times\widehat{\mathbb{Z}}$ に拡張して $(\widehat{\mathbb{Z}}\times\widehat{\mathbb{Z}}, \lambda\times\lambda)$ 上の確率変数とすると，次の定理が成り立つのである:

定理 2 (大数の強法則). $\lambda \times \lambda$-a.e. $(x, y) \in \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$ に対して

$$\lim_{N \to \infty} S_N(x, y) = \frac{6}{\pi^2}.$$

ひとたび，大数の強法則が云えたならば，次の目標はそれの精密化である．これは，1つではなくいくつかの道に分かれていて

- 中心極限定理
- 重複大数の法則
- 大偏差原理

などがある．その中で，我々は「中心極限定理スケーリング」，即ち，確率変数列 $\left\{N(S_N(x, y) - \frac{6}{\pi^2})\right\}_{N=1}^{\infty}$ の極限分布について興味をもった．通常の極限定理からの類推より，我々は

「$N(S_N(x, y) - \frac{6}{\pi^2})$ は $N \to \infty$ のとき非退化な正規分布に収束する」

ことを期待した．が，実際はそうはならず，[3] では，まず次のことを示した:

定理 3. $N \in \mathbb{N}$ とする．$L^2(\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}, \lambda \times \lambda)$ の等式として，次式が成り立つ:

$$\begin{aligned} N\left(S_N(x, y) - \frac{6}{\pi^2}\right) = &- \sum_{u=1}^{\infty} \frac{\mu(u)}{u} \left(\frac{(N + x) \bmod u}{u} - \frac{x \bmod u}{u}\right) \\ &- \sum_{u=1}^{\infty} \frac{\mu(u)}{u} \left(\frac{(N + y) \bmod u}{u} - \frac{y \bmod u}{u}\right) \\ &+ \frac{1}{N} \sum_{u=1}^{\infty} \mu(u) \left(\frac{(N + x) \bmod u}{u} - \frac{x \bmod u}{u}\right) \\ &\qquad \times \left(\frac{(N + y) \bmod u}{u} - \frac{y \bmod u}{u}\right). \end{aligned}$$

ここで $\mu : \mathbb{N} \to \{-1, 0, 1\}$ は Möbius 関数，i.e.,

$$\mu(n) = \begin{cases} 1 & n = 1 \text{ のとき}, \\ 0 & n \text{ が平方因子をもつとき}, \\ (-1)^k & n \text{ が相異なる } k \text{ 個の素数の積のとき} \end{cases}$$

である．

簡単のため，上式の右辺を

$$-T(x; N) - T(y; N) + R(x, y; N)$$

とかくことにする．$N \to \infty$ のとき，確かに

$$R(x, y; N) \to 0 \quad \text{in } L^2(\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}, \lambda \times \lambda)$$

となる．ところが，$-T(\cdot;N)$ は普通の意味では収束しない．"$N \to \infty$" に適当な付帯条件を付けることにより，$-T(\cdot;N)$, よって $N(S_N(x,y)-\frac{6}{\pi^2})$ は，意味のある極限をもつことが分かるのである．

このことを詳述するため，次を用意する：

定義 4. $\widehat{\mathbb{Z}}$ に同値関係 "$\sim$" を次のように導入する：

$$z \sim z' \underset{\text{def}}{\iff} (z-z') \bmod p = 0, \quad {}^{\forall}p\text{: 素数}.$$

いつものように $z \in \widehat{\mathbb{Z}}$ の属する同値類を $[z]$ とかく．$\widehat{\mathbb{Z}}/\!\sim$ を商位相空間とすると，これは距離化可能で，結果 compact 距離空間となる．

定義 5. $T(\cdot;N)$ を拡張して

$$T(x;z) = \sum_{u=1}^{\infty} \frac{\mu(u)}{u}\left(\frac{(z+x) \bmod u}{u} - \frac{x \bmod u}{u}\right)$$

とおく．これは L^2 収束し，写像

$$\widehat{\mathbb{Z}} \ni z \mapsto T(\cdot;z) \in L^2(\widehat{\mathbb{Z}},\lambda)$$

は連続となる．さらに

- $z, z' \in \widehat{\mathbb{Z}}$ に対して

$$T(\cdot;z) = T(\cdot;z') \text{ in } L^2(\widehat{\mathbb{Z}},\lambda) \underset{\text{iff}}{\iff} z \sim z',$$

- 一般に点列 $\{z^{(k)}\}_{k=1}^{\infty} \subset \widehat{\mathbb{Z}}$ と $z \in \widehat{\mathbb{Z}}$ に対して

$$T(\cdot;z^{(k)}) \to T(\cdot;z) \text{ in } L^2(\widehat{\mathbb{Z}},\lambda) \underset{\text{iff}}{\iff} [z^{(k)}] \to [z] \text{ in } \widehat{\mathbb{Z}}/\!\sim$$

が成り立つことが分かる．よって，各同値類 $[z]$ に対して

$$T(\cdot;[z]) := T(\cdot;z)$$

とおく．

さて，次が [3] の主結果である：

定理 4 (中心極限定理スケーリング極限). $\left\{N(S_N(x,y)-\frac{6}{\pi^2})\right\}_{N\in\mathbb{N}}$ の $L^2(\widehat{\mathbb{Z}}\times\widehat{\mathbb{Z}},\lambda\times\lambda)$ における集積点全体の集合は

$$\left\{-T(x;[z]) - T(y;[z])\,;\,[z] \in \widehat{\mathbb{Z}}/\!\sim\right\}$$

である．さらに，各 $[z] \in \widehat{\mathbb{Z}}/\!\sim$ に対して

$$\lim_{N\to\infty \text{ with } [N]\to[z] \text{ in } \widehat{\mathbb{Z}}/\sim} N\left(S_N(x,y) - \frac{6}{\pi^2}\right) = -T(x;[z]) - T(y;[z]) \quad \text{in } L^2(\widehat{\mathbb{Z}}\times\widehat{\mathbb{Z}},\lambda\times\lambda).$$

2. 杉田の予想

定理 4, 及び $T(\cdot;[0])=0$ より, 自然数列 $\{N_k\}_{k=1}^{\infty}$ が

$$[N_k]\to[0]\quad \text{in } \widehat{\mathbb{Z}}/\sim \ \text{ as } k\to\infty,$$

云い換えると

$$^{\forall}p\text{: 素数に対して } {}^{\exists}k_p\in\mathbb{N}\ \text{ s.t. } p|N_k \ \text{ for } {}^{\forall}k\geq k_p \tag{1}$$

をみたすとき,

$$\lim_{k\to\infty}N_k\Big(S_{N_k}(x,y)-\frac{6}{\pi^2}\Big)=0\quad \text{in } L^2(\widehat{\mathbb{Z}}\times\widehat{\mathbb{Z}},\lambda\times\lambda)$$

となる. これは,

「$S_{N_k}(x,y)-\frac{6}{\pi^2}$ を $\frac{1}{N_k}$ で normalize したものは, $k\to\infty$ のとき自明なものに収束する」

と主張する. では,

「$\{\frac{1}{N_k}\}$ より速くゼロに収束するもので normalize したら, 自明でないものに収束するだろうか?」

この問いのため, 定理 3 にある式を $T(x;N)+T(y;N)$ の L^2-norm で割ってみる:

$$\frac{N\Big(S_N(x,y)-\frac{6}{\pi^2}\Big)}{\sqrt{2}\|T(\cdot;N)\|_2}=-\frac{1}{\sqrt{2}}\left(\frac{T(x;N)}{\|T(\cdot;N)\|_2}+\frac{T(y;N)}{\|T(\cdot;N)\|_2}\right)+\frac{R(x,y;N)}{\sqrt{2}\|T(\cdot;N)\|_2}.$$

このとき, 右辺の第 2 項は negligible, i.e., $\{N_k\}_{k=1}^{\infty}$ が (1) をみたすとき

$$\lim_{k\to\infty}\frac{R(x,y;N_k)}{\|T(\cdot;N_k)\|_2}=0\quad \text{in } L^2(\widehat{\mathbb{Z}}\times\widehat{\mathbb{Z}},\lambda\times\lambda)$$

となることが分かる. 右辺の第 1 項について, 杉田は次を予想した:

予想. $\{N_k\}_{k=1}^{\infty}$ が (1) をみたすならば

$$\frac{T(x;N_k)}{\|T(\cdot;N_k)\|_2}\Rightarrow\mathfrak{N}(0,1)\quad \text{as } k\to\infty.$$

ここで $\mathfrak{N}(0,1)$ は標準正規分布を表わす.

この予想と上のことを合わせれば

「$S_{N_k}(x,y)-\frac{6}{\pi^2}$ を $\frac{\sqrt{2}\|T(\cdot;N_k)\|_2}{N_k}$ で normalize したものは, $k\to\infty$ のとき $\mathfrak{N}(0,1)$ に収束する」

が従うのである (これはあくまでも予想を認めた上での話である^^;).

3. 数値実験による予想の検証

まず，定義 5 で述べなかったことを注意しておく:

注意 1. ${}^\forall z \in \widehat{\mathbb{Z}}$, $1 \le {}^\forall r < \infty$ に対して $T(\cdot; z)$ は L^r 収束する．

このことから $T(\cdot; z)$ はすべてのモーメントをもつので，「杉田の予想」を証明する 1 つの方策として次を採る: ${}^\forall m \in \mathbb{N}$ に対して

$$\lim_{k\to\infty} \mathbf{E}^\lambda\left[\left(\frac{T(x;N_k)}{\|T(\cdot;N_k)\|_{L^2}}\right)^{2m-1}\right] = 0,\quad \lim_{k\to\infty} \mathbf{E}^\lambda\left[\left(\frac{T(x;N_k)}{\|T(\cdot;N_k)\|_{L^2}}\right)^{2m}\right] = \frac{(2m)!}{2^m m!}.$$

しかし，今のところ，この収束を示すことに成功していない．そこで，まず初めの一歩として，このことを数値実験により確かめることにした．

我々の数値実験の方法は次のとおりである:
まず，$-T(x;N)$ を次の有限級数で近似する:

$$-T_{10000}(x;N) := \sum_{u=2}^{10000} \frac{\mu(u)}{u}\left(\frac{(x+N) \bmod u}{u} - \frac{x \bmod u}{u}\right).$$

そして，$-T_{10000}(x;N)$ のサンプルを $0 \le x \le 2^{62}-1$ の範囲から 10^7 個だけ，random Weyl sampling (cf. [2]) によって生成する．

具体的には，最初にランダムに $0 \le x', \alpha' \le 2^{124}-1$ を選び (無理数回転による疑似乱数生成法を用いる (cf. [1]))，次に $n = 1, 2, \ldots 10^7$ に対して

$$x'_n := (x' + n\alpha') \bmod 2^{124}$$

とし，

$$x_n := \left\lfloor \frac{x'_n}{2^{62}} \right\rfloor$$

を x のサンプルとする．つまり，$\{-T_{10000}(x_n;N)\}_{n=1}^{10^7}$ を実験に用いるサンプルとするのである．

k 次モーメントの実験値を

$$v^{(k)}(N) = \frac{1}{10^7}\sum_{n=1}^{10^7}(-T_{10000}(x_n;N))^k$$

とし，$T(\cdot;N)$ の標準偏差 $\sigma(N) = \|T(\cdot;N)\|_2$ は

$$\sigma(N)^2 = \sum_{i,j=1}^{\infty} \mu(i)\mu(j)\frac{(i,j)^2}{i^2 j^2}\frac{N \bmod (i,j)}{(i,j)}\left(1 - \frac{N \bmod (i,j)}{(i,j)}\right)$$

(ここで $(i,j) = \gcd(i,j)$) となるから，$\sigma(N)$ を次の近似式で計算する:

$$\sigma_{10000}(N)^2 := \sum_{i,j=1}^{10000} \mu(i)\mu(j)\frac{(i,j)^2}{i^2j^2}\frac{N \bmod (i,j)}{(i,j)}\left(1 - \frac{N \bmod (i,j)}{(i,j)}\right).$$

そして $v^{(k)}(N)$ と $\sigma_{10000}(N)$ の比

$$r^{(k)}(N) = \frac{v^{(k)}(N)}{\sigma_{10000}(N)}$$

を考えるのである．

我々は (1) をみたす $\{N_k\}_{k=1}^{\infty}$ として，簡単のため

$$N_k = p_1 \cdots p_k$$

を採ることにする．これの $k = 1, 2, \ldots, 13$ のときの値は次のようになる:

$$\begin{aligned}
N_1 &= 2,\\
N_2 &= 6,\\
N_3 &= 30,\\
N_4 &= 210,\\
N_5 &= 2310,\\
N_6 &= 30030,\\
N_7 &= 510510,\\
N_8 &= 9699690,\\
N_9 &= 223092870,\\
N_{10} &= 6469693230,\\
N_{11} &= 200560490130,\\
N_{12} &= 7420738134810,\\
N_{13} &= 304250263527210.
\end{aligned}$$

N_k は非常に速く無限大に発散することが見てとれる．実際，素数定理より $N_k = k^{(1+o(1))k}$ as $k \to \infty$ となっている．

さて，我々の数値計算の結果は次のとおりである:

N	N_4	N_5	N_6	N_7
$r^{(1)}$	6.4598489×10^{-6}	$-1.0435065 \times 10^{-5}$	$-5.8815538 \times 10^{-6}$	$-3.6578590 \times 10^{-6}$
$r^{(2)}$	1.0001529	1.0000312	1.0002163	1.0002075
$r^{(3)}$	$-1.9050199 \times 10^{-1}$	1.7332654×10^{-1}	$-3.1382850 \times 10^{-2}$	$-1.6890768 \times 10^{-3}$
$r^{(4)}$	2.9583985	2.9573068	2.8886984	3.0112429
$r^{(5)}$	-1.7683383	1.5543094	$-2.5076080 \times 10^{-1}$	$-2.7438590 \times 10^{-2}$
$r^{(6)}$	1.4652466×10	1.4499693×10	1.3413212×10	1.5136741×10
$r^{(7)}$	-1.7000258×10	1.4497850×10	-2.0289523	$-3.7560895 \times 10^{-1}$
$r^{(8)}$	1.0304908×10^2	9.9525119×10	8.4248418×10	1.0666222×10^2

N	N_8	N_9	N_{10}	N_{11}
$r^{(1)}$	6.5760434×10^{-6}	$-9.6921078 \times 10^{-6}$	$-1.6507803 \times 10^{-5}$	6.3804749×10^{-8}
$r^{(2)}$	9.9989659×10^{-1}	1.0001852	9.9990277×10^{-1}	9.9986182×10^{-1}
$r^{(3)}$	5.9224527×10^{-2}	$-5.1096359 \times 10^{-3}$	1.1598020×10^{-1}	1.1331084×10^{-2}
$r^{(4)}$	2.9695540	2.9924840	2.9886225	2.9385676
$r^{(5)}$	5.1433825×10^{-1}	$-9.3139504 \times 10^{-2}$	1.0937986	1.0499755×10^{-1}
$r^{(6)}$	1.4539306×10	1.4819750×10	1.4929763×10	1.4124994×10
$r^{(7)}$	4.6494245	-1.3263030	1.0816388×10	1.0484380
$r^{(8)}$	9.8405046×10	1.0179075×10^2	1.0517468×10^2	9.3413680×10

N	N_{12}	N_{13}
$r^{(1)}$	2.8926173×10^{-6}	$-1.3930030 \times 10^{-5}$
$r^{(2)}$	9.9987113×10^{-1}	9.9985483×10^{-1}
$r^{(3)}$	$-2.1054763 \times 10^{-2}$	$-1.3490485 \times 10^{-2}$
$r^{(4)}$	2.9975423	2.9554136
$r^{(5)}$	$-2.1649597 \times 10^{-1}$	$-1.2843073 \times 10^{-1}$
$r^{(6)}$	1.4956986×10	1.4376460×10
$r^{(7)}$	-2.3003951	-1.2816008
$r^{(8)}$	1.0433597×10^2	9.6793523×10

$r^{(k)}$ の理想値は

$$r^{(2m-1)} = 0,\ r^{(2m)} = \frac{(2m)!}{2^m m!}$$

である ($r^{(4)} = 3$, $r^{(6)} = 15$, $r^{(8)} = 105$ となる). これと上の結果を比較するならば，我々の実験は「杉田の予想」を否定はしていない，どちらかと云えば支持している，と思える．この実験結果を頼りとして，「予想」を数学的に証明して「定理」に格上げすること，これが，これからの我々のやるべき仕事ということになる．

参考文献

[1] H. Sugita, Pseudo-random number generator by means of irrational rotation, *Monte Carlo Methods and Appl.*, **1** (1995), pp. 35–57.

[2] H. Sugita and S. Takanobu, Random Weyl sampling for robust numerical integration of complicated functions, *Monte Carlo Methods and Appl.*, **6** (2000), pp. 27–48.

[3] H. Sugita and S. Takanobu, The probability of two integers to be co-prime, revisited — law of large numbers and its refinement, Preprint (2001).